

IEEE Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances

IEEE Electromagnetic Compatibility Society

Developed by the
Standards Development and Education Committee

IEEE Std 1848™-2020

STANDARDS

IEEE Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances

Developed by the

**Standards Development and Education Committee
of the
IEEE Electromagnetic Compatibility Society**

Approved 4 June 2020

IEEE SA Standards Board

Abstract: A set of practical methods is provided for helping to manage the levels of risks due to electromagnetic (EM) disturbances throughout the lifecycles of electronic equipment. These risks include the consequences of all types of errors, malfunctions, or failures in products, equipment, and systems that employ modern electronic technologies (i.e., in hardware and/or software).

The work done in creating IEC 61000-1-2:2016 (Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology is supplemented by this standard for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena) by providing requirements for detailed practical techniques and measures for helping to manage risks (not just functional safety) that could be caused by EM disturbances.

These techniques and measures would be used in the management, specification, design, implementation, verification and validation, and through-life operation, maintenance, repair, refurbishment, upgrading, and eventual dismantling for disposal of equipment and systems employing digital electronic systems, for both hardware and software (firmware).

Keywords: digital systems, electromagnetic interference, EMI, electromagnetic compatibility, EMC, electromagnetic disturbances, functional safety, IEEE 1848™, risk management, risk reduction

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

Copyright © 2021 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 27 April 2021. Printed in the United States of America.

IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-1-5044-6750-6 STD24215
Print: ISBN 978-1-5044-6751-3 STDPD24215

IEEE prohibits discrimination, harassment, and bullying.

For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE Standards documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page (<https://standards.ieee.org/ipr/disclaimers.html>), appear in all standards and may be found under the heading “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE SA) Standards Board. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA, and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

IEEE makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. IEEE standards documents are supplied “AS IS” and “WITH ALL FAULTS.”

Use of an IEEE standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity, nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: THE NEED TO PROCURE SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE is the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, consulting information, or advice pertaining to IEEE Standards documents.**

Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive the concurrence of a balance of interests. For this reason, IEEE and the members of its Societies and Standards Coordinating Committees are not able to provide an instant response to comments, or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the [IEEE SA myProject system](#). An IEEE Account is needed to access the application.

Comments on standards should be submitted using the [Contact Us](#) form.

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document does not constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

Copyrights

IEEE draft and approved standards are copyrighted by IEEE under US and international copyright laws. They are made available by IEEE and are adopted for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400; <https://www.copyright.com/>. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Updating of IEEE Standards documents

Users of IEEE Standards documents should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect.

Every IEEE standard is subjected to review at least every 10 years. When a document is more than 10 years old and has not undergone a revision process, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE standard.

In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit [IEEE Xplore](#) or [contact IEEE](#). For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the [IEEE SA Website](#). Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the Additional Resources Details section. Errata are also available in [IEEE Xplore](#). Users are encouraged to periodically check for errata.

Patents

IEEE Standards are developed in compliance with the [IEEE SA Patent Policy](#).

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the

IEEE SA Website at <https://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

IMPORTANT NOTICE

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. IEEE Standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

Participants

At the time this IEEE standard was completed, the IEEE 1848 Working Group had the following membership:

Keith Armstrong, *Chair*
Alistair Duffy, *Vice Chair*

Luk Arnaut
Christine Blair
Kai Borgeest
Tom Braxton
Niklas Briest
Harald Buchwald
Felix Burghardt
Johan Catrysse
Junhong Deng
Pete Dorey
Lionel Doris
Eric Easton
Radu Gosav

Hrvoje Grganic
Greg Hiltz
Richard Hoad
Elya Joffe
Brian Kirk
Matthias Kreitlow
Jong Hwa Kwon
Yeou Song Lee
Damian Lopez
Ken Lynch
Murray T. Marple
Adrian Monk
Nicholas Monk

Doug Nix
Tim Peikert
Davy Pisssoort
Hugo Pues
William Radasky
Frank Sabath
Carlos Sartori
Curt Sponberg
Ken Webb
Warwick Wong
Richard Worley
Nicholas Zagrodnik
Steve Zerenner

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

William Ackerman
Robert Aiello
Martin Armstrong
William Bloethe
Bill Brown
Demetrio Bucaneg Jr.
William Bush
William Byrd
Carole Carey
Ross Carlton
Juan Carreon
Suresh Channarasappa
Ashley Chappell
Keith Chow
Paul Croll
Ernest Duckworth
Alistair Duffy
Sourav Dutta
Craig Fanning
David Fuschi
James Gilb
Randall C. Groves

John Harauz
Timothy Harrington
Werner Hoelzl
Daniel Hoolihan
Sergiu Iordanescu
Atsushi Ito
Efthymios Karabetsos
Kenneth Karg
Sheldon Kennedy
Yuri Khersonsky
Thomas Koshy
Jim Kulchisky
Thomas Kurihara
Robert Landman
Yeou Song Lee
Arthur H. Light
John MacDonald
Jose Marrero
Andrew Nack
Ghery Pettit
Jan Pirrong
Davy Pisssoort

Iulian Profir
Hugo Pues
Beth Pumo
William Radasky
Moises Ramos
Lakshman Raut
Charles Rogers
Bartien Sayogo
Jerry Smith
Gary Smullin
Thomas Starai
John Stevens
Gary Stodter
Walter Struppler
Thomas Tullia
David Turner
Mark-Rene Uchida
John Vergis
Robert Wilken
Oren Yuen
Marc Zeidman
Shuhui Zhang

When the IEEE-SA Standards Board approved this standard on 4 June 2020, it had the following membership:

Gary Hoffman, *Chair*
Jon Walter Rosdahl, *Vice Chair*
John D. Kulick, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edward
J. Travis Griffith
Grace Gu
Guido R. Hiertz
Joseph L. Koepfinger*
David J. Law

Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Dorothy Stanley

Mehmet Ulema
Lei Wang
Sha Wei
Philip B. Winston
Daidi Zhong
Jingyi Zhou

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 1848-2020, IEEE Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances.

This IEEE Standard provides guidance on the assessment and application of techniques and measures that can help reduce the risks associated with the interfering effects of electromagnetic disturbances on digital electronic systems, especially safety- or mission-related systems.

When competently selected and applied, a set of such techniques and measures can provide the part of the evidence relevant to EMI required for justifying functional safety decisions and for compliance with functional safety standards (including all applicable parts of IEC 61508 Ed.2:2010 or functional safety standards that are based on IEC 61508).¹

The scope of this standard does not cover human health effects caused by electromagnetic fields (EMF); HERF (Hazards of Electromagnetic Radiation to Fuel); or HERO (Hazards of Electromagnetic Radiation to Ordnance).

Beneficial comments (recommendations, additions, deletions) and any pertinent data that may be of use in improving this document should be addressed to IEEE, EMC Society, Standards Development and Education Committee, and P1848 Working Group.

A committee consisting of representatives of academia, government, and industry prepared this document under the IEEE EMC Society Standards Development and Education Committee.

¹ Information on references can be found in Clause 2.

Contents

1. Overview	12
1.1 Scope	13
1.2 Purpose	13
1.3 How to use this standard.....	13
1.4 The relationship between this IEEE Standard and IET 2017 [B8]	13
2. Normative references.....	15
3. Definitions	16
4. General introduction to the techniques and measures for achieving electromagnetic resilience	21
4.1 Overview	21
4.2 Why manage risks due to electromagnetic disturbances?.....	21
4.3 The aims and application of this standard.....	24
4.4 Relationship with IEC 61508:2010 and other safety standards	24
4.5 Achieving electromagnetic resilience for functional safety.....	25
4.6 Application of electromagnetic resilience techniques and measures	29
4.7 Assessment of electromagnetic resilience techniques and measures	30
4.8 Documentation of electromagnetic resilience.....	32
5. Checklist of electromagnetic resilience techniques and measures.....	33
Annex A (informative) Detailed guidance on electromagnetic resilience techniques and measures.....	51
A.1 Electromagnetic resilience in project management, planning, and specification.....	51
A.2 Electromagnetic resilience techniques and measures for use in system design	56
A.3 Techniques and measures for use in operational design	69
A.4 Techniques and measures for implementation, integration, installation and commissioning	99
A.5 Techniques and measures for verification and validation (including testing).....	102
A.6 Techniques and measures for operation, maintenance, repair, overhaul, refurbishment, and upgrade	107
A.7 Maintaining electromagnetic resilience during decommissioning.....	111
A.8 Integrating third-party items into safety-related systems.....	112
Annex B (informative) Bibliography.....	115
B.1 General references	115
B.2 Good EMC engineering for systems and installations	116
B.3 Good EMC engineering for individual items of equipment.....	118
B.4 Software design techniques and measures	119
B.5 IEC and CISPR standardized EMC test methods.....	122
B.6 Automotive industry EMC test standards	124
B.7 Marine industry EMC test standards.....	125
B.8 Undersea industry EMC test standards	125
B.9 Rail industry EMC standards and guidance documents.....	126
B.10 Civilian avionics and aerospace industry EMC test standards	128
B.11 Military industry EMC test standards	128
B.12 ITE, Telecommunications and Wireless industry EMC test standards	129
B.13 Some ‘ad hoc’ test methods	129
B.14 Assessing the electromagnetic environment and detecting threats	130
B.15 Verification/validation and other techniques (not specifically related to electromagnetic disturbances).....	131
B.16 References associated with Annex E	135

Annex C (informative) Some functional safety standards based on applicable parts of IEC 61508	137
Annex D (informative) Glossary	139
Annex E (informative) General concepts and definitions of 'Risk'	140
E.1 Different kinds of Risk	140
E.2 Managing functional safety (and other) risks due to EMI	144
E.3 Examples of techniques and measures for EM resilience	145
Annex F (informative) Comparison with IEC standard	147
Annex G (informative) Cross-references between the reference numbering in this IEEE standard and that in IET 2017 [B8]	153
G.1 General references, cross-reference list	153
G.2 Good EMC engineering for systems and installations, cross-reference list	154
G.3 Good EMC engineering for individual items of equipment, cross-reference list	154
G.4 Software design techniques and measures, cross-reference list	155
G.5 IEC and CISPR standardized EMC test methods, cross-reference list	156
G.6 Automotive industry EMC test standards, cross-reference list	157
G.7 Marine industry EMC test standards, cross-reference list	157
G.8 Undersea industry EMC test standards, cross-reference list	157
G.9 Rail industry EMC standards and guidance documents, cross-reference list	158
G.10 Civilian avionics and aerospace industry EMC test standards, cross-reference list	159
G.11 Military industry EMC test standards, cross-reference list	159
G.12 ITE, Telecommunications and Wireless industry EMC test standards, cross-reference list	159
G.13 Some 'ad hoc' test methods, cross-reference list	160
G.14 Assessing the electromagnetic environment, and detecting threats, cross-reference list	160
G.15 Verification/validation and other techniques (not specifically related to electromagnetic disturbances), cross-reference list	160
G.16 References associated with Annex E, cross-reference list	162

IEEE Standard for Techniques and Measures to Manage Functional Safety and Other Risks with Regard to Electromagnetic Disturbances

1. Overview

This IEEE Standard provides guidance on the assessment and application of techniques and measures that can reduce the risks associated with the interfering effects of electromagnetic disturbances on digital electronic systems, especially safety- or mission-related systems.

When competently selected and applied, a set of such techniques and measures can provide the part of the evidence relevant to EMI required for justifying functional safety decisions and for compliance with functional safety standards (including all applicable parts of IEC 61508 Ed.2:2010 or functional safety standards that are based on IEC 61508; see the partial list in Annex C).

They can also provide part of the evidence relevant to EMI for medical/healthcare systems for which risks are managed in accordance with ISO 14971:2007 [B11].²

This standard supports the adoption of adequate electromagnetic resilience engineering practices throughout the functional safety lifecycle by offering further guidance and practical advice on the application of risk management activities, including the techniques and measures set out in IEC 61000-1-2:2016.

While it is primarily intended to be used by those who have responsibilities for functional safety, the methodologies, techniques, and measures it describes can also be used for the reduction of other kinds of risks in any systems that employ electronic technology, such as security risks and non-safety-related risks (for example, risks to the operation of commercial IT systems). However, this standard does not address the risks to human health that can be caused by electromagnetic fields (EMF); HERF (Hazards of Electromagnetic Radiation to Fuel); or HERO (Hazards of Electromagnetic Radiation to Ordnance).

² The numbers in brackets correspond to those of the bibliography in Annex B.

1.1 Scope

This standard provides a set of practical methods for managing functional safety and other risks due to electromagnetic (EM) disturbances throughout the life of a product.

This includes all types of errors, malfunctions or failures in products, equipment, and systems that employ modern digital technologies (i.e., hardware and software).

1.2 Purpose

The purpose of this standard is to provide requirements for the techniques and measures used in the design, verification, and validation of systems, hardware, and software (firmware).

These would be applied where EM disturbances could cause errors, malfunctions, or failures leading to unacceptable risks over the lifetime of equipment, whether safety or any other kind of risk is to be managed.

1.3 How to use this standard

This standard requires a structured justification of adequate electromagnetic resilience of a system to be individually provided for each safety function in that system, following the approach taken by the IEC's Basic Standard on Functional Safety, IEC 61508.

Clause 4 describes the use of this standard in detail, and the required structured justification for each of a system's safety functions is achieved by completing the cells in the right-hand-most column of the checklist in Clause 5 plus providing all the documents referenced in those cells.

In general, it is expected that most systems requiring safety risk management will have several safety functions, each one of which will be associated with its own, completed, Clause 5 checklist. In some circumstances, two or more different safety functions may be able to be addressed by a single Clause 5 checklist.

IEC 61508 provides a well-proven process for assessing functional safety-related risks and by how much they need reduction (its SILs 1-4), and then it prescribes the well-proven techniques and measures that shall or should be employed to reducing those risks to the extent required. Unfortunately, neither it nor its 'daughter' standards (see the partial list in Annex C) contains a complete set of techniques and measures suitable for reducing the functional safety risks due to EM disturbances to the extent required.

This standard relies on IEC 61508's hazard analysis and risk assessment process having been completed as part of the overall risk management of functional safety for a system, and merely adds the missing techniques and measures necessary for fully controlling the functional safety risks that could be affected by EM disturbances.

1.4 The relationship between this IEEE Standard and IET 2017 [B8]

These two documents are closely related. Because the risk management of EM disturbances is such a new field, a conscious effort was made by the IEEE's working group to keep the texts of the two documents identical as far as possible.

The reasons for this were to minimize the possibilities for accidentally causing confusion by describing the same thing in two different ways, as well as to minimize the increase in functional safety (or other) risks that could foreseeably be caused in projects (especially multinational projects) in which some people are using IET 2017 [B8] and some are using this standard.

It has not been possible to keep the reference numbering—for example: [B999]—identical between IET 2017 [B8] and this standard, so a new Annex G has been added in this standard to provide cross-references between them. Throughout the text of this standard, reference numbers in square brackets are linked to their relevant cross-reference lists in Annex G by text or a footnote.

The cross-reference tables in Annex G should make it easy for anything referenced in this standard to be correlated with the same thing in IET 2017 [B8], to help avoid confusion in geographically diverse project teams when some members might be using IET 2017 [B8] while others are using this standard.

Another significant difference concerns the normative checklist in Clause 5 of this IEEE Standard. In IET 2017 [B8], this checklist is merely a recording convenience in its informative Annex A, whereas in this IEEE Standard, it is a *normative* requirement in Clause 5.

This change has caused some knock-on renumbering of clauses and subclauses in this standard, so they no longer correspond directly with IET 2017 [B8], as follows. In Annex A of this standard, the numbering is identical to that in Clause 2 of IET 2017 [B8] *except that* the first character in the numbering in *this* standard is the letter A (e.g., A.3.2), whereas in IET 2017 [B8], it is the number 2 (e.g., 2.3.2).

Finally, because this IEEE Standard is a newer document than IET 2017 [B8], some of its contents have been slightly changed from those in IET 2017 [B8] in order to clarify their meanings without changing them. Also, some of the contents of this IEEE Standard are new and additional to the contents of IET 2017 [B8].

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they shall be understood and used, so each referenced document is cited in the text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE/ANSI C63.14™-2014, American National Standard Dictionary of Electromagnetic Compatibility (EMC) including Electromagnetic Environmental Effects (E3).^{3, 4}

IEC 61000-1-2:2016, Electromagnetic compatibility (EMC) - Part 1-2: General - Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena (an IEC Basic Safety standard as defined in IEC Guide 104).^{5, 6}

IEC 61508-1 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 1: General requirements.⁷

IEC 61508-2 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 2: Requirements for electrical/electronic/programmable electronic safety related systems.

IEC 61508-3 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3: Software requirements.

IEC 61508-4 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 4: Definitions and abbreviations.

IEC 61508-5 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 5: Examples of methods for the determination of safety integrity levels.

IEC 61508-6 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3.

IEC 61508-7 Ed. 2.0, Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 7: Overview of techniques and measures.⁸

³ ANSI publications are available from the American National Standards Institute (<http://www.ansi.org/>). IEEE publications are available from The Institute of Electrical and Electronics Engineers (<http://standards.ieee.org/>).

⁴ The IEEE standards or products referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.

⁵ For the corresponding reference number in IET 2017 [B8], see Annex G.

⁶ IEC publications are available from the International Electrotechnical Commission (<http://www.iec.ch>) and the American National Standards Institute (<http://www.ansi.org/>).

⁷ For the corresponding reference number in IET 2017 [B8], see Annex G.

⁸ For the corresponding reference number in IET 2017 [B8], see Annex G.

3. Definitions

For the purposes of this document, the following terms and definitions apply. The *IEEE Standards Dictionary Online* and IEEE/ANSI C63.14-2014 should be consulted for terms not defined in this clause.⁹ The glossary in Annex D may also be useful.

3.1 A: ‘Amperes’.

3.2 AC: ‘Alternating current’, a term used to denote electrical power or signals that are at a frequency other than 0 Hz.

3.3 Amp: Abbreviation of Ampere, the standard unit of measuring electrical current flow.

3.4 Anticipated lifecycle: The ‘safety lifecycle’ that is anticipated by the risk management process at the planning stage.

3.5 Availability: The probability of functioning at a given instant.

3.6 CE marking: A form of mark that indicates that a product is claimed by its supplier to comply with all relevant EU Directives, such as the EMC Directive.¹⁰

3.7 Competence: Having the training, technical knowledge, experience, and qualifications relevant to the specific duties to be performed. (Adapted from IEC 61508-1; for more details, see IEC 61508-1 Ed.2:2010, subclauses 6.2.13 to 6.2.15.)

3.8 Competent: Having the appropriate competence relevant to the specific duties to be performed. (Adapted from IEC 61508-1; for more details, see IEC 61508-1 Ed.2:2010, subclauses 6.2.13 to 6.2.15.)

3.9 Conducted transients: Conducted emissions that are transient (short term) in their nature, such as ‘spikes’, usually described in time-domain terms, for example, as a waveform, rather than in frequency-domain terms, such as a spectrum.

3.10 Conducted: When applied to emissions or immunity, this term refers to unwanted electromagnetic energy conducted from equipment via the power supply or data, signal, or control conductors.

3.11 DC: ‘Direct current’, a term used to denote an electrical power or signal voltage or current at 0 Hz.

3.12 Dropout: A sudden reduction of the electrical power supply voltage to zero for a short period of time, usually less than 1 s, followed by a recovery to the original level.

3.13 DS: ‘Defined state’, an equipment ‘performance criterion’: a specified, detectable operational state that an element or subsystem of a safety-related system switches to, temporarily or permanently, within a stated time, if it suffers from errors, malfunctions, or failures, for example, from EMI during an immunity test. Destruction of components is allowed as long as the DS of the EUT is maintained or achieved within a stated time. See 3.1.21 in IEC 61000-1-2:2016. Some EMC publications related to functional safety used to use the abbreviation ‘FS’ for this performance criterion instead of ‘DS’.

⁹ *IEEE Standards Dictionary Online* is available at: <http://dictionary.ieee.org>. An IEEE Account is required for access to the dictionary, and one can be created at no charge on the dictionary sign-in page.

¹⁰ For the corresponding reference number in IET 2017 [B8], see Annex G.

3.14 EDR: Event data recorder, a nonvolatile memory that stores ‘events’ detected by programmed diagnostic techniques, such as errors or failures, whether or not they were associated with a safety incident/accident.

3.15 Electromagnetic field: As an electromagnetic wave propagates in three-dimensional space and time, the magnitudes of its electric and magnetic waves can be represented as varying fields within the volume through which it is passing or has passed. Electric field strengths are measured in Volts/meter (V/m) and magnetic field strengths in Amps/meter (A/m).

3.16 Electromagnetic phenomenon: Any type of propagating electromagnetic energy (conducted, radiated, continuous, transient, electric, magnetic, voltage, current, common mode, differential mode, antenna mode, arc or spark, etc.) or a change in the propagating medium itself.

3.17 Element: A part of a system comprising a single component or any group of components that performs one or more element safety functions.

NOTE 1—An element may comprise hardware and/or software.¹¹

NOTE 2—A typical element is a sensor, programmable controller, or final element. (IEC 61000-1-2:2016, definition 3.1.12).

3.18 EMC Directive: Legal instrument by which all member states in the European Union (EU) are obliged to enact national laws that have the same effect, to restrict the supply of electrical and electronic goods in the EU to those that meet certain minimum requirements for electromagnetic emissions and immunity.

NOTE—See [B1].¹²

3.19 Equipment: A general term that refers to a wide variety of possible elements, modules, devices, and assemblies of products (see IEC 61000-1-2:2016, definition 3.1.14).

3.20 ETSI: European Telecommunications Standards Institute. (See <http://www.etsi.org>)

3.21 EUC: ‘Equipment under control’, equipment, machinery, apparatus, or plant used for manufacturing, process, transportation, medical or other activities, including the EUC’s control systems (See IEC 61508-4, definition 3.2.1, modified.)

3.22 Field: See electromagnetic field.

3.23 Filter: A combination of capacitors, inductors, RF absorbers, resistors, and/or other types of components intended to reduce the amount of electromagnetic energy at certain frequencies from being conducted along a cable or wire.

¹¹ Notes in text, tables, and figures of a standard are given for information only and do not contain requirements needed to implement this standard.

¹² For the corresponding reference number in IET 2017 [B8], see Annex G.

3.24 FPGA: ‘Field-programmable gate array’, an integrated circuit designed to be configured by a customer or a designer after manufacturing—hence ‘field-programmable’. The FPGA configuration is generally specified using a hardware description language (HDL), similar to that used for an application-specific integrated circuit (ASIC). (Circuit diagrams were previously used to specify the configuration, as they were for ASICs, but this is increasingly rare.) FPGAs contain an array of programmable logic blocks, and a hierarchy of reconfigurable interconnects that allow the blocks to be ‘wired together’, like many logic gates that can be inter-wired in different configurations. Logic blocks can be configured to perform complex combinational functions or merely simple logic gates like AND and XOR. In most FPGAs, logic blocks also include memory elements, which may be simple flip-flops or more complete blocks of memory. (From Wikipedia: https://en.wikipedia.org/wiki/Field-programmable_gate_array.)

3.25 Functional safety: That part of the overall safety that depends on the correct functioning of electrical, electromechanical, or electronic (hardware and software) technologies.

3.26 HR: ‘Highly recommended’.

3.27 I/O: Input/output.

3.28 IC: ‘Integrated circuit’, a type of semiconductor device that contains many transistors, arranged to provide certain electronic functions. The latest types of IC can contain several million individual transistors.

3.29 IEMI: ‘Intentional electromagnetic interference’, intentional malicious generation of electromagnetic energy introducing noise or signals into electric and electronic systems, thus disrupting, confusing, or damaging those systems for terrorist or criminal purposes. (Taken from IEC 61000-2-13:2004.)

3.30 IET: The Institution of Engineering and Technology, created in 2006 by the merger of the Institution of Electrical Engineers (IEE, which dates back to 1884) with the Institution of Incorporated Engineers (IIE). Based in London, U.K.

3.31 Interference: Usually shorthand for ‘electromagnetic interference’, also known as EMI or RFI.

3.32 Jammer: A jamming device (‘jammer’) is a radio frequency transmitter that intentionally blocks, jams, or interferes with communications such as cell phone calls, text messages, GPS systems, and IEEE 802.11 networks. (See <https://www.gps.gov/spectrum/jamming/>)

3.33 Jamming: The act of using a jamming device or ‘jammer’ to intentionally block, jam, or interfere with lawful communications such as cell phone calls, text messages, GPS systems, and IEEE 802.11 networks. (See <https://www.gps.gov/spectrum/jamming/>)

3.34 JTAG: IEEE Std 1149.1™-1990, Standard Test Access Port and Boundary-Scan Architecture.

3.35 Lifecycle: A period of time that starts at the concept phase of a project and finishes when all of the safety-related systems and other risk reduction measures are no longer available for use. (See IEC 61508-4, definition 3.7.1; excerpt modified.)

3.36 Lightning protection: Protection against the direct and/or indirect effects of lightning.

3.37 Liveness: In concurrent computing, liveness refers to properties of concurrent systems that require a system to make progress despite the fact that its concurrently executing components (processes) may have to ‘take turns’ in critical sections, parts of the program that cannot be simultaneously run by multiple processes. Liveness guarantees are important properties in operating systems and distributed systems.

NOTE—(See [B126].¹³)

3.38 Packet sequencing: ‘A powerful tool that uses the Sequenced Packet Protocol (SPP): a networking protocol that provides reliable transport of packets with flow control in environments where multiple transport connections are established. SPP uses destination ID reference numbers to identify the target end of a transport connection; sequence numbers to keep transmitted packets in the order in which they were sent; and acknowledge numbers that are assigned to the last packet in a sequence that a destination received properly to indicate that the transmission is complete and successful.’

(From http://www.webopedia.com/TERM/S/sequenced_packet_protocol.html.)

3.39 PCB: ‘Printed circuit board’, laminated structure with layers of etched foil conductors (usually copper) known as tracks or traces, interspersed with layers of dielectrics (often a glass-fiber matrix). Sometimes called a printed wiring board (PWB). The traces are interconnected between layers by plated-through holes (PTH) known as ‘via holes’. Electronic components are mounted onto the PCB and soldered to the traces on the outermost layer(s). Components with long pins or leads may be connected directly to traces on inner layers by plated through holes.

3.40 Power quality: A general term embracing a number of issues affecting the quality of the AC or DC electrical power supply, such as dips, dropouts, interruptions, sags, swells, harmonic waveform distortion, inter-harmonic waveform distortion, surges, spikes, and transients. The standard for instruments measuring power quality is IEC 61000-4-30.

3.41 Reliability: The probability of functioning properly over a given period of time.

3.42 Resilience: The capacity to recover quickly or easily from difficulties, misfortune, or change; toughness.

3.43 Resilient: Having resilience.

3.44 RF Reference: A conductive structure, usually a continuous or meshed (gridded) metal sheet or volume; in installations usually a meshed structure made of interconnected conductors and metal structures that maintains a low impedance (generally much less than $1\ \Omega$) up to some defined frequency.

3.45 Safety case: A structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a safety-related system is safe enough for a given application in a given environment.

3.46 Safety documentation: Includes all the information necessary for the safe use of the item. Safety manuals and safety cases are examples of such documentation.

3.47 Safety function: A function to be implemented by an Electrical/Electronic/Programmable Electronic safety-related system or other risk reduction measures that is intended to achieve or maintain a safe state for the EUC, in respect of a specific hazardous event.

Examples of safety functions include functions that are required to be carried out as positive actions to avoid hazardous situations (for example switching off a motor) and functions that prevent actions being taken (for example preventing a motor starting). (From IEC 61508-4, definition 3.5.1.)

3.48 Safety integrity level: A discrete level (one out of a possible four), corresponding to a range of safety integrity values, where safety integrity level 4 has the highest safety integrity level and safety integrity level 1 has the lowest. The target failure measures for the four safety integrity levels are specified in Tables 2 and 3 of IEC 61508-1. (See IEC 61508-4, definition 3.5.8.)

¹³ For the corresponding reference number in IET 2017 [B8], see Annex G.

3.49 Safety lifecycle: The necessary activities involved in the implementation of safety-related systems, occurring during a period of time that starts at the concept phase of a project and finishes when all of the E/E/PE safety-related systems and other risk reduction measures are no longer available for use.

NOTE 1—The term ‘functional safety lifecycle’ is more accurate, but the adjective ‘functional’ is not considered necessary in this case within the context of this document.

NOTE 2— The safety lifecycle models used in this document are specified in Figures 2, 3, and 4 of IEC 61508-1. (See IEC 61508-4, definition 3.7.1.)

3.50 Safety manual: For compliant items, a document that provides all the information relating to the functional safety of an element, in respect of specified element safety functions, that is required to help ensure that the system meets the requirements of IEC 61508 series. (See IEC 61508-4:2010, definition 3.8.17.)

3.51 Safety: Freedom from unacceptable risk. (See ISO/IEC Guide 51:1999, definition 3.1.)

3.52 Safety-related system: The designated system that both implements the required safety functions necessary to achieve or maintain a safe state for the EUC and is intended to achieve, on its own or with other safety-related systems and other risk reduction measures, the necessary safety integrity for the required safety functions. (See IEC 61508-4, definition 3.4.1.)

3.53 SC: Systematic capability.

3.54 Screening: An alternative term for shielding.

3.55 SIL: See ‘Safety integrity level’.

3.56 Surge: A type of transient voltage and/or current with a high energy content, typically produced by the energy associated with a lightning strike or flyback of stored inductive energy (for example, in a large electric motor or generator) coupling into cables such as power supply or telecommunication cables. A surge is generally considered to have much longer rise times and decay times, as well as to have much more energy associated with it, than a ‘transient’, ‘fast transient’, or ‘spike’.

3.57 Systematic capability: The measure (expressed on a scale of SC 1 to SC 4) of the confidence that the systematic safety integrity of an element meets the requirements of the specified SIL, in respect of the specified element safety function, when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

NOTE 1—Systematic capability is determined with reference to the requirements for the avoidance and control of systematic faults (see IEC 61508-2 and IEC 61508-3).

NOTE 2—What is a relevant systematic failure mechanism will depend on the nature of the element. For example, for an element comprising solely software, only software failure mechanisms will need to be considered. For an element comprising hardware and software, it will be necessary to consider both systematic hardware and software failure mechanisms.

NOTE 3—A Systematic capability of SC N for an element, in respect of the specified element safety function, means that the systematic safety integrity of SIL N has been met when the element is applied in accordance with the instructions specified in the compliant item safety manual for the element.

3.58 Wave: A physical quantity (e.g., voltage current, or field strength) that fluctuates with time and/or distance.

3.59 Waveform: The two-dimensional shape made by a plot or graph of a physical quantity (e.g., voltage, current, or field strength) when it is plotted or displayed on the vertical axis, with time or distance on the horizontal axis. *Syn:* **Wave shape, waveshape**

4. General introduction to the techniques and measures for achieving electromagnetic resilience

4.1 Overview

This standard provides guidance on the assessment and application of techniques and measures that can help reduce the risks associated with the interfering effects of electromagnetic disturbances on digital electronic systems, especially safety- and mission-related systems.

When competently selected and applied, a set of such techniques and measures will provide the part of the evidence relating to EMI, required for justifying functional safety decisions and for compliance with functional safety standards (including all applicable parts of IEC 61508 Ed.2:2010 or functional safety standards that are based on IEC 61508:2010).

The expectation is that compliance with this standard will be achieved by adding text and links to other design, verification, or validation documents into the cells in the right-hand-most column of one or more copies of the checklists in Clause 5 to demonstrate whether and how each technique or measure has been applied for each of a system's safety functions.

The scope of this standard does not cover human health effects caused by electromagnetic fields (EMF); HERF (Hazards of Electromagnetic Radiation to Fuel); or HERO (Hazards of Electromagnetic Radiation to Ordnance).

4.2 Why manage risks due to electromagnetic disturbances?

All electronic and electro-mechanical technologies can suffer errors, malfunctions, or failures due to electromagnetic interference (EMI), which can be caused by electromagnetic disturbances. For nonsafety equipment, functionality in this regard is generally demonstrated by compliance with all applicable electromagnetic immunity test standards.

Where electronic or electro-mechanical technologies are used in a safety-related application, it is necessary to ensure that EMI cannot cause safety risks to exceed tolerable limits. However, compliance with electromagnetic immunity test standards (for example, those listed as providing a presumption of conformity to the EMC Directive [B1]¹⁴) does not demonstrate safety performance, and traditional immunity testing cannot validate equipment's safety performance to the confidence required for safety applications.

In practice, a number of factors related to electromagnetic disturbances limit the confidence with which safety performance can be demonstrated, including:

- a) Over a lifecycle, in any real situation the characteristics and locations of sources of electromagnetic disturbances can rarely be known with confidence, and often cannot be predicted with complete confidence.
- b) Operational experience is of very limited value in demonstrating safety performance with respect to EMI throughout the operation of a safety-related system. Errors, malfunctions, and failures caused by EMI are often transitory, leaving no tangible evidence of their occurrence, making fault identification and evidence gathering extremely difficult unless specific techniques and measures are used.
- c) No practicable amount of electromagnetic immunity testing can be sufficient, on its own, to demonstrate the performance of a safety component or system throughout its life.

¹⁴ For the corresponding reference number in IET 2017 [B8], see Annex G.

The likelihood of EMI impacting the performance of safety-related systems is also increasing because:

- d) There is a rapidly increasing use of wireless systems, high-speed and/or high-power switching devices, and programmable electronics, in all applications. The electromagnetic disturbances increasingly being emitted by these technologies, and their increasing use, will make the electromagnetic environment progressively worse, in terms of noise levels, spectral density, and bandwidth for the foreseeable future.
- e) Modern safety systems increasingly employ technologies with the potential for decreased immunity (increased susceptibility), for example, modern electronics operating at lower switching voltages, lower power consumption, and wireless receivers. The application of such technologies may not be evident without detailed analysis of product design information.
- f) The use of intentionally generated electromagnetic disturbances to prevent the operation of a system is a growing concern, not just for the military sector but also for critical infrastructure and other sectors.

Consequently, there is a need to manage the electromagnetic resilience of safety systems, in order to help ensure that they are capable of delivering their intended risk reduction throughout their operation.

The basic IEC publication covering electromagnetic compatibility (EMC) for functional safety is IEC 61000-1-2:2016. This publication establishes a methodology that may contribute to the achievement of functional safety as regards the effects of electromagnetic phenomena for electrical and electronic systems and installations.

IEC 61000-1-2:2016 uses the terminology of IEC 61508:2010 and can be used to support claims, made in accordance with the applicable parts of IEC 61508:2010 and functional safety standards based upon it, that functional safety has been achieved with regard to electromagnetic disturbances.

The methodology set out in IEC 61000-1-2:2016 is based on risk management principles and focuses on reducing risks throughout the lifecycle of a safety-related system. However, it is used as a framework for this standard based on good engineering practices in managing risks. Table 3 and Annex B within that standard briefly describe a number of techniques and measures related to electromagnetic resilience—the subject of this standard—as being a practical method for helping to achieve compliance. Figure 1 provides an overview of the use of IEC 61000-1-2 from a management perspective.

The medical industry uses IEC 60601-1-2 Ed.4:2014 (see Annex C) to manage the risks that can be caused by electromagnetic disturbances.

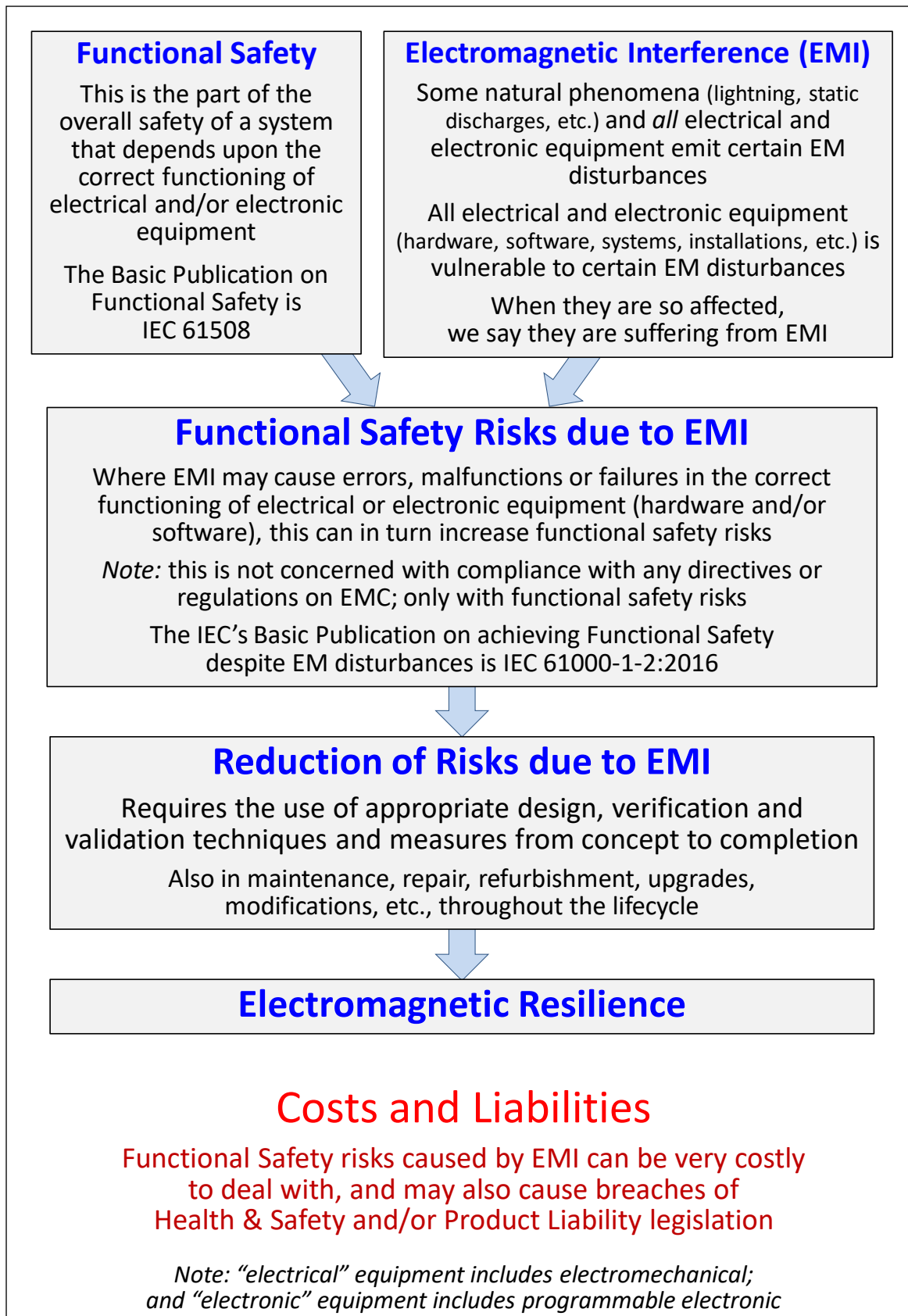


Figure 1—Overview of electromagnetic resilience issues (source: IET 2017 [B8])

4.3 The aims and application of this standard

The aim of this standard is to support the achievement of functional safety performance by providing guidance on the selection and application of electromagnetic resilience techniques and measures.

Its purpose is to support the adoption of adequate electromagnetic resilience engineering practices throughout the functional safety lifecycle by offering further guidance and practical advice on the application of risk management activities, including the techniques and measures set out in IEC 61000-1-2:2016.

This standard is intended to be used by those who have responsibilities for functional safety. While it is aimed at functional safety, the methodologies, techniques, and measures described here can also be used for the reduction of other risks, such as security risks and non-safety-related risks (for example, risks to the operation of commercial IT systems).

4.4 Relationship with IEC 61508:2010 and other safety standards

Designers of systems have a professional obligation to be aware of relevant safety standards and comply with them at the current state of the art.

This standard supplements the information on dealing with EMI given in all applicable parts of IEC 61508:2010 and other standards or specifications containing electromagnetic requirements for functional safety, such as IEC 61000-1-2, IEC 61326-3-1 [B4]¹⁵, IEC 61326-3-2 [B5]¹⁵, IEC 61000-6-7 [B3]¹⁵, and IEC 60601-1-2 (see Annex C).

This standard also updates and adds to the information in the IET's 2008 and 2013 guides [B7]¹⁵, as well as in the IET's 2017 Code of Practice on Electromagnetic Resilience [B8] on which it is based.

NOTE—All editions of IEC 61326-3-1 and IEC 61326-3-2 up to and including their 2017 editions are not considered complete 'EMC for functional safety' standards because they are not based on IEC 61000-1-2, which is the IEC's basic standard on this topic.

The situation regarding electromagnetic disturbances and functional safety was not well understood when the basic safety standard IEC 61508 was first published in 2000, or when the functional safety standards based upon IEC 61508 were first published (see Annex C).

The result is that, generally, the EMC requirements in those standards are currently based upon a restricted set of standard laboratory tests, applied only to representative examples of equipment, which cannot provide sufficient confidence that safety-related systems, or the subsystems or elements they incorporate, will not suffer intolerable risks because of EMI throughout the lifecycle.

IEC 61000-1-2 Ed.1:2016 was created specifically to provide the electromagnetic requirements that are missing from such standards. The relevant parts of IEC 61508:2010 list an early version, IEC TS 61000-1-2:2008, as a normative reference.

IEC 61000-1-2:2016 is intended by its authoring committee to complement all applicable parts of IEC 61508:2010. It provides guidance on how electromagnetic engineering may contribute to the achievement of functional safety because this area is not covered in detail in the applicable parts of IEC 61508:2010. IEC 61000-1-2:2016 is a basic safety standard and, like IEC 61508:2010, is intended to be used by the authors of other functional safety standards as the technical basis for the requirements in the standards they create.

¹⁵ For the corresponding reference number in IET 2017 [B8], see Annex G.

IEC 61000-1-2:2016 describes the situation regarding electromagnetic disturbances and the achievement of functional safety, and its Annex B describes electromagnetic resilience. It includes practical techniques and measures for helping to ensure that electromagnetic disturbances do not cause functional safety risks to exceed tolerable levels, based upon the IET's 2013 guidance [B7]¹⁶.

The relationship of this standard to IEC and ISO standards has been described above. Where IEC and ISO standards have been adapted to fulfil national or Trade Bloc regulatory purposes (for example, when prefixed with EN, ANSI, etc., or completely renumbered), this standard can be considered to be relevant to them in the same way.

4.5 Achieving electromagnetic resilience for functional safety

The methodology set out in IEC 61000-1-2 (and, for medical devices, in IEC 60601-1-2, see Annex C) is based on risk management principles and focuses on reducing risks due to electromagnetic disturbances throughout the entire lifecycle, from concept to end of life. The approach taken by this standard is illustrated in Figure 2.

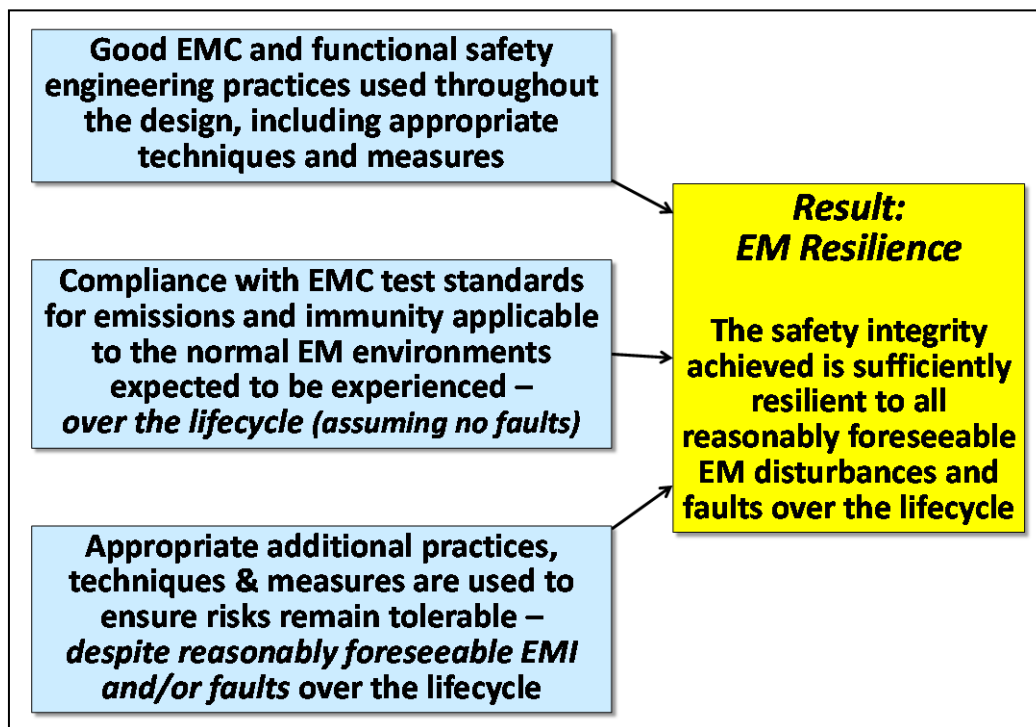


Figure 2—Achieving electromagnetic resilience (source: IET 2017 [B8])

The intention is to support architectures and designs that are inherently resilient to electromagnetic disturbances.

¹⁶ For the corresponding reference number in IET 2017 [B8], see Annex G.

The approach shown in Figure 2 builds on the existing competency of the EMC and functional safety engineering communities, as follows:

a. Compliance with EMC standards

EMC design/testing competency, for example, to comply with the EMC Directive [B1]¹⁷, other EMC regulations or customer-specific EMC specifications such as those used by the military, is very well established in the developed world.

The EMC emissions and immunity standards that are used have been developed over the years (and are still developing) for the purpose of ensuring adequate availability of equipment/system functionality, with different standards being developed to suit the wide variety of generalized electromagnetic environments (such as domestic, commercial, light industrial, heavy industrial, military, road vehicles, railways, etc.)

This standard builds on the above experience, competency, and existing EMC test facilities, by recommending that equipment or systems:

- 1) Comply with all published test standards relevant for the electromagnetic disturbances that are expected both to occur in the normal electromagnetic environments and to be experienced by the safety-related system, subsystem, or element.
- 2) Continue to comply with all published relevant test standards throughout their anticipated lifecycles.

NOTE 1—These tests may exceed what is required for EMC Directive compliance, in the number of types of electromagnetic disturbance tested, their levels, and their characteristics (for example, for continuous disturbances: modulation types; frequency ranges; dwell times, etc., and for transient disturbances: wave shapes; number of occurrences, etc.).

NOTE 2—If the electromagnetic environment experienced by the system, subsystem, or element changes over time, these tests should be reviewed to help ensure that the availability of the equipment under control (EUC) remains adequate.

b. The use of electromagnetic resilience techniques and measures

Functional safety requirements should be met over the complete lifecycle, taking into account all reasonably foreseeable:

- 1) Operating conditions
- 2) Errors, malfunctions, and faults, whether static or intermittent, and whether they are random or systematic (i.e., due to the design, sometimes called ‘design-related’ failures)
- 3) Environmental conditions (shock, vibration, humidity, condensation, temperature, electromagnetic disturbances, etc.)
- 4) Wear, corrosion, aging, degradations, and failures
- 5) Component tolerances and variability, construction and installation errors, etc.
- 6) Use and misuse, whether intentional or not
- 7) Multiple electromagnetic disturbances of the same or different types, occurring at the same time or in some critical sequence
- 8) Any combinations of item 1) through item 7) above

Attempting to take all of the above issues into account by EMC testing would take an impractical amount of time and resources, which is why the electromagnetic resilience techniques and measures described in this standard have been developed.

¹⁷ For the corresponding reference number in IET 2017 [B8], see Annex G.

The level of functional safety competency that is required in order to comply with all applicable parts of IEC 61508:2010 and its related standards is well established worldwide. Generally, the techniques and measures employed by these standards are well understood, well proven, and widely used.

These techniques and measures have been developed to help prevent the introduction of systematic errors in the safety-related systems.

Electromagnetic disturbances can also be a cause of errors, malfunctions, or faults in any of the electrical or electronic parts of a safety-related system, and such failures are called electromagnetic interference (EMI). Some techniques and measures that have been widely used to achieve compliance with all applicable parts of IEC 61508:2010 and its related standards may also be partially effective at preventing electromagnetic disturbances from causing EMI that could increase functional safety risks.

This standard builds on the existing experience and competency in the functional safety engineering community by recommending the use of:

- 9) Well-established functional safety techniques and measures that are known to be especially effective against the effects of EMI
- 10) Modifications to certain techniques and measures to make them more effective against the effects of EMI
- 11) Application of good electromagnetic engineering techniques and measures at every level of design (such as components, circuit, PCB, wiring, software, product, element, subsystem and system design, installation design, design for maintainability and repair, etc.) during the anticipated lifecycle
- 12) Application of good electromagnetic engineering practices, including appropriate techniques and measures at every stage of the system lifecycle

IEC 61508:2010 manages the functional safety over the entire lifecycle, and IEC 61000-1-2:2016 gives additional requirements and guidance on functional safety activities relating to electromagnetic disturbances.

This standard recommends compliance with IEC 61000-1-2, including the application of an adequate range of electromagnetic resilience techniques and measures, in order to achieve an appropriate level of electromagnetic resilience. This standard provides expanded guidance on electromagnetic resilience techniques and measures, complementary with that published in Table 3 and Annex B of IEC 61000-1-2:2016.

The selection of techniques and measures employed for a particular system will depend on:

- 13) The technology employed
- 14) The application
- 15) The safety integrity level (SIL) of the system as specified in the applicable parts of IEC 61508:2010, or similar measures of safety integrity such as the ASILs in the applicable parts of ISO 26262

Sufficient assessment shall be carried out to justify the selection of electromagnetic resilience techniques and measures for a safety-related system (see 4.7).

No single technique or measure can be relied upon alone. The functional safety designer will choose a set that helps confirm that—regardless of the electromagnetic disturbances that can cause the errors, malfunctions, or failures—the overall functional safety specifications are met.

As the required level of risk reduction for a safety-related system increases, so does the safety integrity level from, for example, SIL 1 to SIL 4. Demonstrations of adequacy for higher SIL levels will typically involve more developed technical arguments and documentation than those for lower SIL levels. The range of techniques and measures required, as well as the rigor expected from their demonstration, will depend on the situation but will usually increase significantly with each SIL level. A similar approach applies to elements as the systematic capability increases from SC1 to SC4.

The competent application of a set of electromagnetic resilience techniques and measures (see Annex A) shall be recorded as part of an overall approach to safety documentation based on the principles expressed in the applicable parts of IEC 61508. The safety documentation should demonstrate that there is sufficient confidence that functional safety would not be compromised by electromagnetic disturbances over the anticipated lifecycle. The adequacy of the overall safety argument expressed in the safety documentation could be subject to independent assessment, where appropriate.

For equipment intended to be used in a safety-related system (for example, subsystems or elements), the competent application of electromagnetic resilience techniques and measures should be recorded in the product's documentation, and made available to system integrators, installers, end users, and assessors as necessary. For example, information related to electromagnetic resilience could be included in the safety manual for compliant items required by the applicable parts of IEC 61508, as well as in safety documentation used for assessing safety-related systems.

4.6 Application of electromagnetic resilience techniques and measures

This standard describes a range of techniques and measures that are considered to be useful, where relevant, for improving the electromagnetic resilience during all stages in the safety-related system or safety-related product lifecycle (see Figure 3).

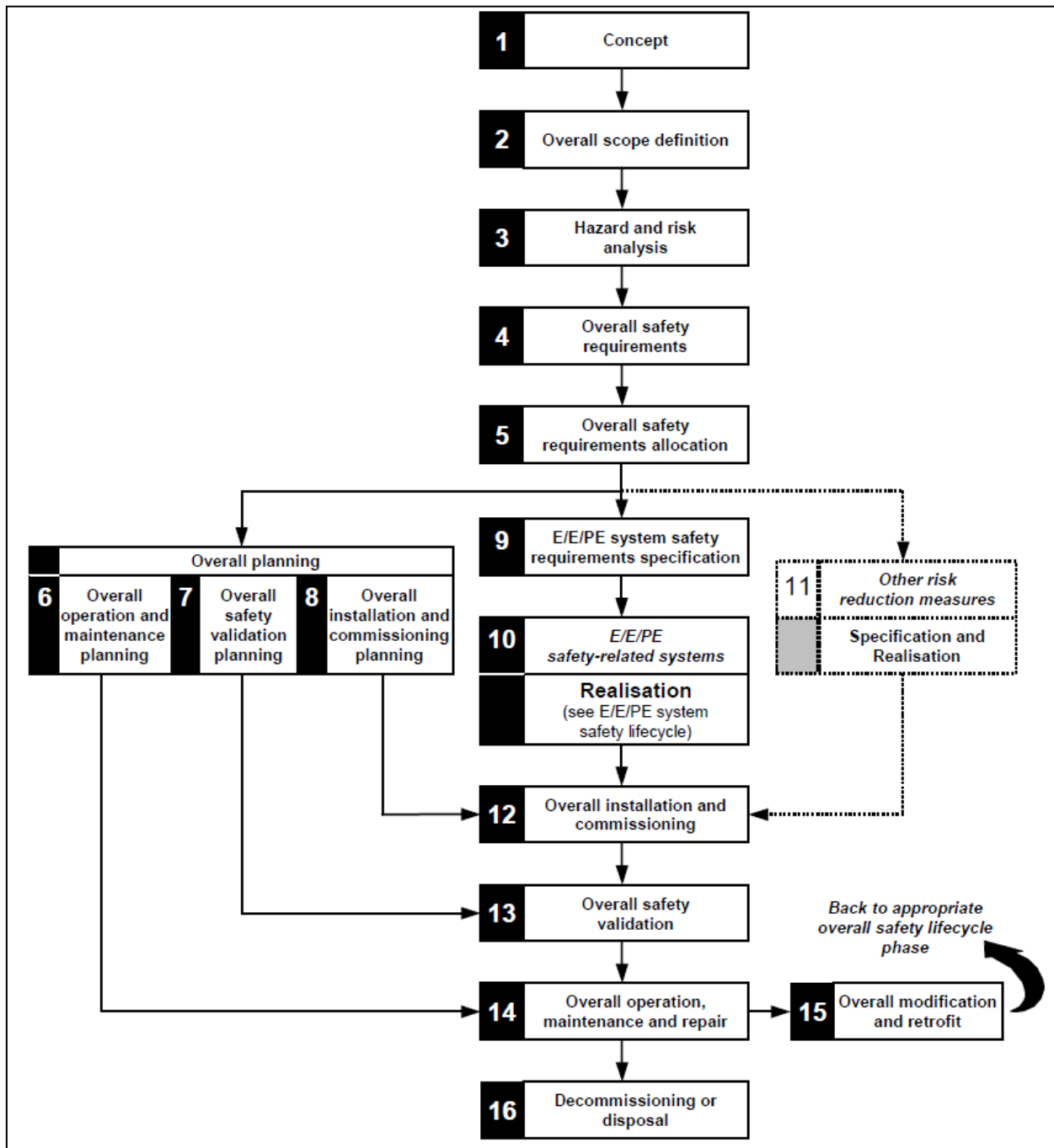


Figure 3—Overview of the functional safety lifecycle (source: IEC 61508-1:2010)

Applicable parts of IEC 61508:2010 require all functional safety-related projects to consider all these stages, whether they concern the creation of equipment for use in constructing a safety-related system (usually standard products manufactured in volume) or the integration or creation of a safety-related system itself.

Activities shall be identified and employed to deliver sufficient electromagnetic resilience for functional safety over the anticipated lifecycle of a safety-related system. These activities shall meet the requirements of relevant functional safety standards and IEC 61000-1-2:2016, and should be applied during the following project stages, as necessary:

- a) Project management, planning and specification
- b) System design
- c) Operational design
- d) System implementation, integration, installation and commissioning
- e) Verification and validation, including through-life monitoring
- f) Operation, maintenance, repair, overhaul, refurbishment, upgrade as necessary
- g) Decommissioning as necessary

These activities should be identified, managed, and documented in line with the standards expected for other aspects of functional safety, and should therefore be allocated to competent persons.

Responsibilities for the achievement of functional safety should therefore be identified. This should include the identification of responsibilities for ensuring adequate electromagnetic resilience of the safety-related system or product.

Clause 5 is a checklist of the electromagnetic resilience techniques and measures that are described in detail in Annex A of this standard. This checklist includes columns detailing their importance versus their safety integrity level or safety capability.

4.7 Assessment of electromagnetic resilience techniques and measures

As part of functional safety lifecycle management activities, appropriate arrangements shall be made to select and implement a suitable range of techniques and measures for electromagnetic resilience.

An adequate combination of techniques and measures shall be selected that, together, achieve the required safety integrity level/systematic capability with respect to electromagnetic disturbances. Their selection shall be recorded within the safety documentation. It is recommended that an assessment of the necessary techniques and measures should be prepared. Adequate reasons should be recorded for the selections made and for rejecting those that are not used. Clause 5 in this standard provides a basic checklist that shall be applied for this purpose.

Annex A of this standard identifies a number of techniques and measures that may be employed at appropriate stages of the system lifecycle as necessary. However, those applied need not be limited to those given in this standard—additional techniques and measures may give added assurance of electromagnetic resilience.

No electromagnetic resilience techniques and measures, such as those described in this standard, should be assumed to guarantee complete protection against every possible type of electromagnetic disturbance, combination of electromagnetic disturbances, faults, or misuse that could result in EMI.

The exact combination of techniques and measures selected for a particular application will depend on many factors specific to the application in question. Except where stated otherwise, the techniques and measures covered by this standard are appropriate for both ‘continuous’ and ‘on-demand’ safety functions.

Depending on the nature of the project, different electromagnetic resilience techniques and measures might be used in its various stages:

- a) If a project did not involve any software design, then no software design techniques and measures would be selected for any of the project's stages.
- b) Likewise, if there was no circuit design required, then circuit design techniques and measures are not needed.

The extent to which robust conventional electromagnetic compatibility (EMC) management techniques (such as high-specification electromagnetic mitigation including shielding, filtering, and transient suppression) can prevent electromagnetic disturbances from affecting the correct operation of a safety-related system during its anticipated lifecycle may be taken into account during the selection and application of the techniques and measures, where this is justified.

Each of the techniques or measures described in Annex A of this standard is presented based on its relevance to the stage of the project, under the following headings: Aim, Description, Identification, Mitigation, and Importance.

Aim	The overall purpose of the technique or measure.		
Description	Broadly how the technique or measure achieves its aim.		
Identification	The effectiveness of the technique or measure to reveal the presence of an error or malfunction that could be caused by electromagnetic disturbances.		
Mitigation	The behavior of the system safety function in response to the detected errors or malfunctions that could have been caused by electromagnetic disturbances.		
Importance	Specifies the necessity and/or desirability of the technique or measure for reducing the risks due to electromagnetic disturbances using the attributes, as follows:		
	Not Recommended (NR)	Recommended (R)	
	Highly Recommended (HR)	Mandatory (M)	
	In this standard, the Importance of a technique or measure as NR, R, HR, or M (see above) is graded according to the relevant safety integrity level (SIL) as specified in the applicable parts of IEC 61508:2010 or similar measures of safety integrity specified in a related functional safety or risk management standard.		

Parts 1 and 5 of IEC 61508:2010 describe its methodology for determining the safety integrity level of a safety function, and other functional safety or risk management standards will have equivalent methodologies. Also see Annex D in Part 7 of IEC 61508:2010.

In accordance with the methodology used in IEC 61508:2010, if a technique or measure rated as HR for the relevant safety integrity level/systematic capability is not used, a detailed technical explanation of why not should be included in the relevant safety documentation. For example, the technique or measure might not actually be relevant for the design being implemented, or it might be that an alternative technique or measure is used instead, which provides the same benefits for risk-reduction to the design issue concerned.

Notes to consider when reading this standard

NOTE 1—For clarity, the Importance for each technique and measure is only shown in the checklist table in Clause 5.

NOTE 2—Where a technique or measure in A.2 or A.3 applies to a technology that is not relevant to the equipment or system concerned, and the importance as shown in Clause 5 as being M or HR, a justification for why that technique or measure was not applied should be included in the safety documentation (see 4.8).

NOTE 3—The Importance levels (R, HR, M) listed in Clause 5 are generic starting points, and an informed application consistent with expectations of the relevant sector should be made. For example, in certain industries (e.g., rail, military, or nuclear) where Clause 5 lists importance as R they might expect HR or M; and where Clause 5 lists HR they might expect M.

4.8 Documentation of electromagnetic resilience

4.8.1 Documentation of electromagnetic resilience for safety-related systems

In the case of a complete safety-related system, the safety documentation should contain all the necessary evidence that shows that the overall safety-related system is adequate for its required safety duty.

Prior to the safety-related system being put into use, a structured justification of adequate electromagnetic resilience of the system shall be produced. This justification could be assessed as part of functional safety assessment activities; alternatively, other appropriate structured assessment approaches could be used.

This justification should assess the extent of compliance with the requirements of relevant functional safety standards including IEC 61000-1-2:2016, and the adequacy of the range of activities, techniques, and measures employed for electromagnetic resilience, including verification and validation activities.

Supporting information should be available for this justification as necessary, and this will usually include electromagnetic environment specifications, electromagnetic tests results and certifications, and material demonstrating the range and suitability of the electromagnetic resilience techniques and measures used in the safety lifecycle.

Information used to support claims made as to the safety performance of a safety-related system should be made available to system integrators and end users and should be retained in order to support system review activities throughout the lifecycle of the system.

Independent assessment of the electromagnetic resilience justification should be undertaken where appropriate. The extent of independence required for assessment should be in line with the approach suggested for independent assessment in the applicable parts of IEC 61508-1:2010.

The expectation is that compliance with this standard will be achieved by adding text and hyperlinked references to other design, verification, or validation documents, into the cells in the right-hand-most columns of the checklist in Clause 5, to demonstrate whether and how each of the techniques or measures have been applied to each safety function.

For safety systems having more than one safety function, it is usually necessary to consider the range of techniques and measures applied from the perspective of each safety function in turn. However, some techniques and measures may apply across more than one safety function, and the presentation of justifications for these may be able to avoid repetition by being covered by a single checklist from Clause 5, as long as this can be done without losing clarity.

As discussed in 4.7, if a technique or measure in the checklist in Clause 5 is categorized as HR for the level of safety integrity appropriate for the safety function in question, but has not been applied, the right-hand-most column will communicate the reasons why not, and what was done instead.

The structured justification of adequate electromagnetic resilience of a system is expected to be provided for all of the safety functions in that system, by one or more copies of the checklist in Clause 5, with their right-hand-most columns duly completed, plus all of the documents referenced in those columns.

4.8.2 Documentation of electromagnetic resilience for equipment (e.g., system elements)

In the case of equipment intended for use in a safety-related system, where electromagnetic resilience claims are made for the equipment, information supporting these claims shall be made available in the compliant item's safety manual.

This should include information that will be required by the safety-related system integrator, for example, the safety-related environmental tests that the equipment complies with, the functional safety techniques and measures that have been applied in the design of the equipment, guidance on installation, maintenance etc., as necessary.

A safety manual should also include information on equipment behavior, where appropriate, in the case of failure, for example, 'defined states' (DSs) that the equipment can assume in response to errors or failures due to intolerable EMI, as well as guidance on the application of the equipment.

Information used to support claims made as to the safety performance of a safety-related system element should be made available to system integrators and end users, and should be retained in order to support system review activities throughout the lifecycle of the element's application. Such information might use one or more copies of the checklist in Clause 5, broadly as discussed in 4.8.1, to help to provide a structured justification of its electromagnetic resilience.

5. Checklist of electromagnetic resilience techniques and measures

Complete as many copies of Table 1 below as are needed to cover all of the Safety Functions in the system concerned (see 4.8).

Note that in these tables, the "Refs in this standard" are identical to those in IET 2017 [B8], except that the first character in this standard is the letter A (e.g., A.1.1), whereas in IET 2017 [B8], it is the number 2 (e.g., 2.1.1). Some references in this standard have no counterpart in IET 2017 [B8] because this is a newer document.

Table 1—Checklist of electromagnetic resilience techniques and measures

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
4 & A.1	Techniques and measures in project management, planning, and specification					
4	Establishment of a Risk Management Process A Risk Management Process shall be established for the system concerned, in accordance with the latest version(s) of the most relevant standard(s) based on the applicable parts of IEC 61508:2010 (see Annex C). A competent person shall have the overall responsibility for managing the risks of the system, by employing the Risk Management Process throughout all of its lifecycle stages.	M	M	M	M	
A.1.1	Project management and planning The processes for the management, planning, selection, design, implementation, commissioning, modification verification, and maintenance of each safety function should explicitly include electromagnetic resilience measures and be documented. A competent person should have the overall responsibility for managing the electromagnetic resilience of the system. Appropriate competency should be made available at all lifecycle stages.	M	M	M	M	
A.1.2	Creating a design requirements specification To help confirm that the design specification includes requirements for EMI, and that all reasonably foreseeable electromagnetic disturbances and their effects are taken into account in the specification of the system and its subsystems and elements. Appropriate techniques and measures shall be defined and used to help confirm that the safety-related system shall achieve the required SIL, and all of the subsystems and elements incorporated within it shall achieve their required systematic capabilities, despite any electromagnetic disturbances over the lifecycle. Amongst other issues, the following shall be taken into account: (a) Nonoperation, when operation is required (b) Operation, when no operation is required (c) Unintended or inaccurate operations The specification for electromagnetic resilience techniques and measures shall be (as far as is possible): complete, free from errors and contradictions, and easy to verify.	M	M	M	M	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.1.3	Specifying EMC test standards to help ensure the availability of the EUC To help ensure the availability of the EUC and its safety-related systems, throughout its lifecycle, so that safety-related systems continue to provide safe operation, taking into account availability, throughput rate, production rate, or other financial or mission-critical requirements.	M	M	M	M	
A.1.4	Protecting against high impact, unusual and malicious EMI To help achieve functional safety where high impact, unusual and malicious electromagnetic disturbances could reasonably foreseeably occur and cause temporary disturbance and/or permanent damage to hardware (electronic components, interconnections, etc.).	M	M	M	M	
	Other technique or measure used in project management and planning:	-	-	-	-	
	Other technique or measure used in project management and planning:	-	-	-	-	
	Other technique or measure used in project management and planning:	-	-	-	-	

Table 1—Checklist of electromagnetic resilience techniques and measures (*continued*)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc..
		SIL1	SIL2	SIL3	SIL4	
A.2	Techniques and measures in system design					
A.2.1	Separating safety-related system parts from non-safety-related system parts	HR	HR	HR	HR	
A.2.2	Recording how the design requirements are implemented through design choices	HR	HR	M	M	
A.2.3	Co-design of electromagnetically diverse hardware and software in multiple redundant channels To detect and/or correct systematic failures, using multiple electromagnetically diverse hardware channels and/or software components, to reduce the likelihood that the common-cause characteristics of electromagnetic disturbances will cause an incorrect output to be created.	R	R	HR	HR	
	Hardware and software designers should work together (i.e., co-design) to achieve the required overall diversity in the most effective way in order to meet the requirements of the design requirements specification and its required safety integrity levels and/or systematic capabilities.					
A.2.4	System integration, installation and commissioning To help confirm that electromagnetic resilience is correctly considered when separately tested parts are brought together to form the complete functional system.	HR	HR	M	M	
A.2.5	Fault detection and event data recording for later diagnosis To increase the probability of localizing malfunctions caused by electromagnetic disturbances.	R	R	HR	HR	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.2.6.1	Error detection Redundant data is appended to the actual data using error detection coding (EDC) techniques such as parity or cyclic redundancy checking (CRC) (see A.3.11, A.3.12, and A.3.14), or suitable equivalent EDC techniques, to detect data corruption. Upon detection of data corruption, appropriate action is taken to maintain the safety integrity level/systematic capability, as described in the safety documentation. For example, various retry schemes could be used to improve the reliability of the link (at the expense of overall system performance). Where the safety manual for a subsystem or element includes a DS, it shall provide sufficient detail for correct use by a safety system designer.	HR	HR	HR	HR	
A.2.6.2	Improving the electromagnetic resilience of communication links, by using hardware and/or software techniques to improve the reliability of the links Error correction A variation of error detection using code such that a level of error correction is possible in order to both detect corruption and correct for its effects. Various error correcting code (ECC) schemes (see A.3.11, A.3.12, and A.3.14) can be used to improve the reliability of the link at the expense of reduced data rate. Whenever error correction occurs, this should be logged to aid later diagnosis. See A.2.5.	HR	HR	HR	HR	
A.2.6.3	Protection of a sequence Extra sequence codes can be appended to each packet to enable detection of delayed, lost or duplicated packets. Various techniques and measures in this standard can be used at the packet level, e.g., just a single bit can be alternated between packets to detect a single packet failure (omission or duplication). More elaborate techniques can detect multiple packet failures or corruption.	HR	HR	HR	HR	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.2.6.4	Wireless Mesh Networks Creates multiple geographically diverse wireless datacommunication links to improve the redundancy of datacommunications	R	R	HR	HR	
A.2.7	Synchronization and re-synchronization techniques	R	R	R	R	
A.2.8	Protection from persistent interference by monitoring retry counts	HR	HR	HR	HR	
A.2.9	Independent detection of electromagnetic disturbances and/or EMI	R	R	R	R	
A.2.10	Protection of systems from tampering via communication links to external systems To conserve the safety integrity level/systematic capability of systems, subsystems, or elements that have external communication links, especially with the Internet, at least for electromagnetic resilience.	R	R	HR	M	
A.2.11	Robust, high-specification electromagnetic mitigation Especially useful when degradation or interruption of functionality is not desired.	R	R	R	R	
A.2.12	Techniques and measures to prevent Virtualization of memory and process resources from causing unacceptable risks	R	R	HR	M	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.2.13	Usability engineering	R	R	HR	M	
	Other technique or measure used in system design:	-	-	-	-	
	Other technique or measure used in system design:	-	-	-	-	
	Other technique or measure used in system design:	-	-	-	-	
	Other technique or measure used in system design:	-	-	-	-	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3	Techniques and measures in operational design In the subclauses below, techniques and measures are classified as either hardware or software based, but some may have equivalent representations in either hardware or software which might be more effective in some useful manner.					
A.3.1	Developing appropriate operation and maintenance instructions For procedures that help avoid EMI-induced failures during the operation & maintenance of a safety-related system or a subsystem or element within a safety-related system.	HR	HR	HR	HR	
A.3.2	Designing appropriate maintenance techniques To make it practical to monitor the condition/performance of, and replace if necessary, electromagnetic mitigation items such as filters, surge suppressors, conductive gaskets, etc., which can have a limited operational life.	HR	HR	HR	HR	
A.3.3	Limiting the possibilities for operation and hence for mis-operation. To help avoid EMI causing failures by affecting operator controls.	HR	HR	HR	HR	
A.3.4	Protecting against operator errors, mistakes and other foreseeable misuse	HR	HR	HR	HR	
A.3.5	Protecting against hardware/software modifications or manipulations	HR	HR	HR	HR	
A.3.6.1	Defensive programming techniques To design software programs to detect anomalous control flow, data flow, or data values, which might have been caused by EMI during their execution, and to react in a predetermined and acceptable manner.	Range checking in hardware and in software Range checking the values of all variables (not just I/Os), sometimes called strong data typing. A number of bands are defined for the value of each variable. A typical 3-band example is: (a) Normal operation (b) Warning zone (c) Out of range		R	R	HR
A.3.6.2		Sequence checking Safety functions intended for continuous operation Safety functions intended for on-demand operation		HR	HR	HR
A.3.6.3		Correct rounding and resolution in all calculations		HR	HR	HR
A.3.6.4		Floating point unit and real number arithmetic Help avoid corruption of arithmetic by EM disturbances		HR	HR	M

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.7	Limited use of interrupts To help reduce the impact of corruption due to EMI upon program execution	R	HR	HR	M	
A.3.8	Limited use of memory address pointer variables to reduce impact of memory corruption					
	System-safety functions intended for continuous operation	HR	HR	HR	HR	
	System-safety functions intended for on-demand operation	R	R	R	R	
	Any/all systems with no safe state	M	M	M	M	
A.3.9	Avoiding recursion To help reduce the impact of corruption due to EMI on program execution.	HR	HR	HR	HR	
A.3.10.1	Error detection and correction for invariable memory (i.e., ROM or program memory) Signature of a word or block of data To detect single- and multibit corruption within a block of data. Various checking techniques are available, such as: Cyclic Redundancy Checks (CRC), Secure Hash Algorithm (SHA), and Hamming Codes (for correction as well as detection). Block replication with inversion to detect all bit failures Plus the use of electromagnetically diverse memories to improve effectiveness. Memory boundary protection To prevent incorrect areas being overwritten in the following types of memory: program; stack; statically allocated variables; heap (dynamically allocated variables); inputs, and outputs.	R	R	HR	HR	
A.3.10.2 A.2.3		HR R	HR R	HR HR	HR HR	
A.3.10.3		R	R	HR	HR	
A.3.11		HR	HR	HR	HR	
	Error detection and error correction techniques in redundant designs	R	R	HR	HR	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.12 A.3.11 & A.3.13	Time-based error detection/correction in buses and interfaces to detect transient failures Combine with error checking codes to protect the sequence numbers or time codes.	R	R	HR	HR	
A.3.13.1	Memory testing Before and/or during operation to detect memory-system-specific errors.	R	R	HR	HR	
A.3.13.2	Error detection and error correction for variable memory (e.g., RAM). Detecting failures during addressing, writing, storing and reading data in memory.	R	R	R	R	
A.3.3		HR	HR	HR	HR	
A.3.13.4		R	R	HR	HR	
A.3.14	Error detection/correction in ROM, RAM, buses and interfaces Detects/corrects one or more bit failures in a word.	R	R	HR	HR	
A.3.15.1	Self-test supported by hardware (one-channel)	HR	HR	HR	HR	
A.3.15.2	Coded processing (one-channel)	R	R	R	R	
A.3.15.3	Error detection for logic and data processing units Two or more electromagnetically diverse processing units exchange data (results, intermediate results, and test data) and cross-check at defined 'restore points' from which system operation could be continued in the event of a fault.	HR	HR	HR	HR	
A.3.15.4	Self-test by software during operation	R	R	HR	HR	

Table 1—Checklist of electromagnetic resilience techniques and measures (*continued*)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.16	Error detection and error correction for electrical and electromechanical components To help control failures in components such as relays, actuators, magnetic logic devices etc. When using redundancy, diverse hardware and/or software improves the effectiveness as regards the common-cause effects typical of electromagnetic disturbances.	HR	HR	HR	HR	
A.2.3						
A.3.17	Caution when using hardware or software libraries To help confirm that the electromagnetic resilience measures are applied and verified throughout the whole software design and implementation of a safety related system.	HR	HR	M	M	
A.3.18.1	Testing by redundant hardware To monitor the operation of the relevant function. Using dynamic signaling techniques To detect static failures in communications and processing. Caution with use of test access ports and boundary-scan To prevent any tests/diagnostics from making the system more susceptible to electromagnetic disturbances.	R	R	R	R	
A.3.18.2		R	R	R	R	
A.3.18.3		R	R	R	R	
A.3.18.4		Error detection and correction for electronic components Monitored redundancy Compares the behavior of two or more electromagnetically diverse (see A.2.3) channels. Hardware with automatic self-test To detect faults by periodic checking of the safety functions using automatic self-tests. Analogue signal monitoring To improve confidence in signals and controls.	R	R	HR	HR
A.3.18.5	R		R	R	R	
A.3.18.6	HR		HR	HR	HR	
A.3.18.7	'Data assurance' (content credibility checking) Uses known relationships within a dataset to detect corruption due to EMI.		HR	HR	HR	HR
		R	R	R	R	

Table 1—Checklist of electromagnetic resilience techniques and measures (*continued*)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.19.1	Error detection and correction by monitoring program sequence (i.e., ‘watchdogs’) Watchdog (temporal monitoring) with separate time base without time-window <i>– only to be used if A.3.19.2 or A.3.19.3 below cannot be used.</i> Watchdog (temporal monitoring) with separate time base and time-window Periodically triggered to monitor the computer’s behavior and the plausibility of the program sequence, with both lower and upper time limits set; preferred over A.3.19.1. Logical monitoring of program sequence Monitoring of individual program sections using software (e.g., counting procedure, key procedure) or using external monitoring facilities; preferred over A.3.19.1. Combination of temporal and logical monitoring of program sequences Combining both temporal (with time window) and logical monitoring to retrigger a temporal facility (e.g., an external watchdog) only if the sequence of the program sections is executed correctly. Preferred over A.3.19.1, A.3.19.2, or A.3.19.3 above. Also preferred over both A.3.19.2 and A.3.19.3 used together but independently.	R	R	NR	NR	
A.3.19.2		HR	HR	HR	HR	
A.3.19.3		R	R	HR	HR	
A.3.19.4						
A.3.20	Error detection and error correction by comparing multichannel input/output interfaces Using electromagnetically diverse hardware and/or software To improve the effectiveness of this technique as regards the common-cause effects typical of electromagnetic disturbances, permitting more confident error correction.	R	R	HR	HR	
A.2.3						

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.21	Using test patterns: static and dynamic Using static and dynamic test patterns to detect static failures ('stuck-at' failures) and cross-talk, particularly in input and output units (digital, analogue, serial, or parallel), and to prevent the sending of inadmissible inputs or outputs to the process.	HR	HR	HR	HR	
A.2.3	Using electromagnetically diverse channels To permit more confident error correction.					
A.3.22	Use metal-free fiber-optic cables for signals and data They are intrinsically immune to electromagnetic disturbances.	R	R	R	HR	
A.3.23.1	Techniques for AC and DC power supplies and power converters To detect or tolerate failures caused by degradations or defects in any of the electrical power supplies.	HR	HR	HR	HR	
A.3.23.2	Detecting degradations and defects Various devices and circuit techniques are readily available for detecting any/all defects in AC or DC power supplies.					
A.3.23.3	Power hold-up Using sufficient energy storage (e.g., batteries, supercapacitors, etc.) or back-up power supplies (e.g., generators) with appropriate action taken to maintain the safety integrity/systematic capability when the energy storage runs out.	HR	HR	HR	HR	
A.3.23.4	Detecting excessive radio frequency noise on power supplies Redundant electromagnetically diverse power supplies Using redundant electromagnetically diverse power supplies to continue safe operation by switching from a failed power supply to one that is still operating correctly (e.g., a backup/reserve power supply).	R	R	R	HR	
A.3.24	Monitoring of ventilation, cooling, and heating To detect whether they have been influenced by electromagnetic disturbances.	R	R	HR	HR	
A.3.25	Careful use of wireless (radio) data communications Ensuring that wireless (radio) data communications will not cause an unsafe failure, and will not adversely impact other safety-related parts of the system.	HR	HR	M	M	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.3.26	Good electromagnetic engineering practices used at every level of design To use accepted, good electromagnetic engineering practices at the time of system implementation in order to provide a first line of defense against electromagnetic disturbances.	HR	HR	HR	HR	
A.3.27	Design to comply with EMC test specifications from A.1.3 (and A.1.4 if appropriate) To help ensure that the safety-related system will comply with these EMC test specifications during verification and validation.	M	M	M	M	
A.3.28	De-rating of hardware components, where appropriate To increase the reliability of hardware components, particularly those used for the suppression of electromagnetic disturbances or protection against their effects.	R	R	R	HR	
A.3.29	Improve robustness of interrupts To help reduce the impact of CPU saturation and program execution lock-up due to EMI through interruptions.	HR	HR	M	M	
	Other technique or measure used in operational design:	-	-	-	-	
	Other technique or measure used in operational design:	-	-	-	-	
	Other technique or measure used in operational design:	-	-	-	-	

Table 1—Checklist of electromagnetic resilience techniques and measures (continued)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.4	Techniques and measures in implementation, integration, installation, and commissioning					
A.4.1	Providing information on any constraints and/or additional measures required for installation and commissioning To aid installation and commissioning in accordance with the relevant design requirements for electromagnetic resilience.	HR	HR	HR	HR	
A.4.2	Procure materials, components and products According to their design specifications for achieving electromagnetic resilience.	HR	HR	M	M	
A.4.3	Assemble/integrate according to the electromagnetic resilience design Using the correct materials, components, and products according to their design specifications for achieving electromagnetic resilience.	HR	HR	M	M	
A.4.4	Install/commission according to the design for achieving electromagnetic resilience <i>Also</i> to help ensure that good electromagnetic engineering practices are employed (see A.3.25) as appropriate during installation and commissioning. <i>Also</i> to help ensure that the safety-related system will comply with the EMC test specifications from A.1.3 and (if appropriate) A.1.4 during verification and validation (see A.5.2).	HR	HR	M	M	
	Other technique or measure used for implementation, integration, installation and commissioning:	-	-	-	-	
	Other technique or measure used for implementation, integration, installation and commissioning:	-	-	-	-	
	Other technique or measure used for implementation, integration, installation and commissioning:	-	-	-	-	

Table 1—Checklist of electromagnetic resilience techniques and measures (*continued*)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.5	Techniques and measures in verification and validation (including testing)					
A.5.1	Applying verification, and validation techniques and measures To verify and/or validate as far as is practicable that the design techniques and measures that have been applied function according to the relevant design specification (created by A.1). (Note that EMC testing is covered in A.5.2 and A.5.3.)	M	M	M	M	
A.5.2	Verification testing to the EMC test plan resulting from A.1.3 (and A.1.4 if appropriate)	M	M	M	M	
A.5.3	Using nonstandardized <i>ad hoc</i> checks or tests To help ensure that the safety-related system or any component part of it has sufficient electromagnetic resilience, taking into account the final safety integrity level/systematic capability being aimed for.	HR	HR	HR	HR	
A.5.4	Verifying correct installation and commissioning Having regard to the constraints and additional measures listed as the result of applying A.4.1 and A.4.2, and any others not listed in those subclauses.	HR	HR	HR	M	
A.5.5	EMC tests before and after accelerated life tests To help ensure that EM Resilience is effective during and after accelerated life tests.	R	HR	M	M	
	Other technique or measure used for verification and validation (including testing):	-	-	-	-	
	Other technique or measure used for verification and validation (including testing):	-	-	-	-	
	Other technique or measure used for verification and validation (including testing):	-	-	-	-	

Table 1—Checklist of electromagnetic resilience techniques and measures (*continued*)

Refs in this standard	Overview of the electromagnetic resilience techniques and measures applied to the Safety Function:	Importance (see 4.7)				How applied for this Safety Function? Add all relevant document links, comments, references, etc.
		SIL1	SIL2	SIL3	SIL4	
A.6	Techniques and measures in maintenance, refurbishment, repair, overhaul, modification, upgrade, etc., over the lifecycle					
A.6.1	Assessment of changes in the electromagnetic environment And if necessary modify/upgrade as required so that availability is maintained at a high level (discussed in A.1.3).	HR	HR	HR	M	
A.6.2	Assessment of continuing correct installation Having regard to the constraints and additional measures listed as the result of applying A.4.1, and any others not listed in that subclause.	HR	HR	HR	M	
A.6.3	Maintaining electromagnetic resilience despite modifications or changes Assessing proposed changes to the safety-related system to help ensure that repairs, overhauls, modifications, upgrades, refurbishment, etc. do not unacceptably degrade its electromagnetic resilience.	HR	HR	M	M	
A.6.4	Batch (lot) traceability To help ensure analysis of the root cause of the problem caused by EMI events and containment by identifying product at risk.	HR	HR	M	M	
A.6.5	Component changes, new supplier, dual/alternate source To help preserve electromagnetic resilience design when replacing component due to changes in specifications or process, a reference change, a change of supplier, or obsolescence.	HR	HR	M	M	
	Other technique or measure used for maintenance, refurbishment, repair, modification, upgrade, etc., throughout the lifecycle:	-	-	-	-	
	Other technique or measure used for maintenance, refurbishment, repair, modification, upgrade, etc., throughout the lifecycle:	-	-	-	-	
	Other technique or measure used for maintenance, refurbishment, repair, modification, upgrade, etc., throughout the lifecycle:	-	-	-	-	